"EXPRESS MAIL" Label No. EL140119774
DATE OF DEPOSIT: October 29, 1998

SYSTEM FOR PROTECTION OF GOODS AGAINST COUNTERFEITING

DESCRIPTION

BACKGROUND OF THE INVENTION

Cross-Reference to Related Applications

This application is a continuation-in-part (CIP) of co-pending application Serial No. 09/060,026, filed April 14, 1998. This application is related to Application Serial No. _____ filed October , 1998 by A. Halperin et al (IBM Docket No. YO998-287) entitled "Method and System for Preventing Counterfeiting of High Price Wholesale and Retail Items"; and to Application Serial No._____ filed October , 1998 by A. Afzali-Ardakani et al (IBM Docket No. YO998-342) entitled "Method and System for Preventing Parallel Marketing of Wholesale and Retail Items"; which related Applications are being filed contemporaneously with this application. The entire disclosure of each of these applications is incorporated by reference herein. Each of these three application is copending and commonly assigned.

Field of the Invention

The present invention generally relates to distinguishing authentic goods from counterfeit goods and, more particularly, to a system for authenticating consumer goods using an electronically authenticatable device attached to goods.

Description of the Related Art

Counterfeit or "knock-off" goods costs billions of dollars yearly to companies around the world in lost sales. Many counterfeited products are of inferior quality and therefore may tarnish the reputations of legitimate producers when consumers mistake the counterfeit for the real thing. Even if a counterfeit good is well done, the counterfeiter has avoided any of the expenditures in the research and development or intellectual property concerns incurred by or owed to the legitimate producer. Consumers and producers both suffer from counterfeiting through increased prices for legitimate merchandise and inferior quality of fraudulent merchandise.

Complete prevention against counterfeiting is probably unrealistic, at least for products which are manufactured. Some types of counterfeiting, often of inferior quality, are embraced by some consumers who desire to own, but cannot afford, expensive goods. Also, for products which are easily duplicable with no or little quality loss, some consumers prefer to protect their immediate financial interest rather than the interest of the legitimate producers.

Nevertheless, whether it be for the sake of honesty or because of quality concerns many, if not most, consumers prefer to purchase only authentic merchandise, especially when full price was paid. For these consumers, it is desired to provide a system by which the authenticity of a product can be confirmed to insure that what is being paid for is in fact the real thing.

It has been widely recognized by management of corporations most exposed to counterfeiting, such as, for example, manufacturers of compact disks (CDs), videos,

perfumes, luxury watches, etc., that allowing the public to verify the authenticity of a product with a high degree of certainty would substantially help to mitigate damages incurred from counterfeiters.

Many ingenious anti-counterfeit schemes have been devised over the years. A typical example of a system widely used to identify a counterfeit good involves the use of seals which have traditionally been used to authenticate documents. Variations on this theme include watermarks, such as are found on some international currencies, fine prints, tiny objects attached to a product or the package such as holograms, and so on. The efficacy of such methods has dramatically decreased with the evolution of technology. Due to progress in various technologies, if the customer can recognize the "seal", the counterfeiter usually can imitate it in such a way that the customer cannot detect the difference. For example, holographic seals verifiable by a consumer, once difficult and expensive to reproduce, are now child's play with relatively inexpensive equipment.

On the other hand, it is easy to produce seals only verifiable by the vendor. However, the cooperation of the consuming public to contact the vendor to verify the seal is a drawback. To partially overcome this difficulty, several manufacturers attach a serial number to each item. It has been proposed to improve on this method in U.S. Patent Number 4,463,250 to McNeight et al. and in U.S. Patent Number 5,367,148 Storch et al. For serial numbers to offer increased protection, these patents propose to use a serial number where part or all of the digits are chosen at random or generated by some secret code. The originator keeps a copy of all numbers so generated and the check of authenticity is performed by verifying that the tag of a

given item carries a number on the list. Such methods also propose some partial check using a small computer. Unfortunately, these methods suffer from several drawbacks. First, the need to contact the originator is unavoidable in the prior art. In such case, a counterfeiter may saturate the communication lines used for verification and make the process inefficient. Further, the fact that a database has to be kept of all purchases creates invasion of privacy issues for consumers. For example, if the consumer pays using a credit card, it becomes easy to attach the consumer's name to the product which has been bought, often without the consent of the consumer. Moreover, the originator must keep an ever growing database and must make this database quite secure for an unforeseen amount of time. Every access to the database must be secure, and one has to make certain that no external party obtains access to the database. This of course becomes increasingly difficult the larger and more often the data base is accessed. Secondly, using a small scanner, and the help of several accomplices, a would be counterfeiter may copy huge lists of existing serial numbers if the serial numbers are visible when the product is packaged, and the public has no means by which to even partially authenticate the product prior to purchase if the serial numbers are hidden. This problem is partially due to the fact that there is not very much connection between the serial number and the product it corresponds to, i.e. the serial number does not contain enough information about the product.

Another serious problem related to counterfeiting involves so called "parallel markets". There are two typical scenarios. In the first, stolen new goods can be reintroduced in various markets as genuine new goods, this

is commonly referred to as the "black market". In the second, sometimes referred to as the "grey market", a producer sells on different markets having different pricing policies. An agent in a lower priced market may resell the producer's goods to an agent in a higher priced market. In both cases, the producer loses.

SUMMARY OF THE INVENTION

It is therefore an object of the present invention to help protect legitimate vendors and the public against difficult to recognize counterfeits.

It is yet another object of the present invention to aid law enforcement authorities in the pursuit of counterfeiters and identifying illegal counterfeit goods as well as goods being sold in parallel markets.

It is yet another object of the present invention to provide a system for authenticating goods by using tamper-resistant and/or duplication-resistant electronic "tags" such as smart cards attached to goods.

According to the invention a smart tag attached to the goods contains encrypted authentication information, such as a serial number, and can further contain encrypted identifying information associated with the goods such as, for example, a description of the good's physical appearance or chemical decomposition, its color, its routing information, etc. The encryption procedure comprises public/private key encryption with zero-knowledge protocols. Zero knowledge protocols allow a smart tag to be authenticatable and yet be duplication resistant by allowing the verifying agent to convince him/herself that the smart tag is authentic without revealing its authentication

information.

The verification procedure can be done using a contact or contactless card reader equipped with the appropriate public key and zero-knowledge protocols to decrypt the identifying information. A printed version of the serial number or other authentication information may be placed on the goods in human readable form to quickly verify the information electronically read from the smart tag. With the present invention, only the manufacturer can create such smart tags with the associated data thus making it virtually impossible to pass off a counterfeit good as authentic.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other objects, aspects and advantages will be better understood from the following detailed description of a preferred embodiment of the invention with reference to the drawings, in which:

Figure 1 is a block diagram of a first embodiment of the present invention;

Figure 2 is a sample of a possible serial number structure according to the present invention;

Figure 3 is a block diagram of a second embodiment of the present invention; and

Figure 4 is a block diagram of an embodiment of the invention for identifying parallel markets.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT OF THE INVENTION

Referring now to the drawings, and more particularly to Figure 1 there is shown a block diagram of a first

embodiment of the present invention. A legitimate manufacturer 101 commands a serial number generator 102 to generate sequences of serial numbers. These serial numbers can be just consecutive numbers, or contain uncoded and/or coded information as exemplified in Figure 2. The legitimate manufacturer 101 also possesses private keys, 103 and 104, and the corresponding public keys, 109 and 110, from private key/public key pairs as available now in many forms.

Public key encryption involves the use of private/public key pairs. The private key is known only to the manufacturer. Using a corresponding public key provided by the manufacturer, the consumer or law enforcement agent can verify that the encrypted version matches the serial number. An advantage to this method is that only the manufacturer can produce matching pairs. The wide spread availability of the public key does not compromise the security of the private key. The public key for verification can be made available on the product itself or by the manufacturer for example over the Internet. A comprehensive description on the subject of private/public key pairs and zero-knowledge protocols can be found in "Handbook of Applied Cryptography", Alfred Menezes et al., CRC Press, 1997, and in "Cryptography: theory and practice", D. R. Stinson, CRC Press, 1995, herein incorporated by reference.

Zero knowledge protocols may be used to allow a smart tags to be authenticatable and yet be duplication resistant by allowing the verifying agent to convince him/herself that the smart tag is authentic without the smart tag revealing its authentication information. Such zero knowledge protocols have been disclosed for instance in U. S. Patent 5,140,634 to Guillou et al., U.S. Patent 4,864,110 to Guillou, and U.S. Patent 4,995,082 to Schnorr, all herein

incorporated by reference.

Referring still to Figure 1, the serial number generated by generator 102 is encrypted using the private keys 103 and 104. The serial number and its encrypted version from 103 are communicated to printer-1 at block 105, while the encrypted versions from private key 104 is communicated to smart card writer at block 106. Printer 1 at block 105 prints a visible label 107 and the smart card writer at block 106 produces a smart card 108 containing the coded information prepared at 104. The visible label is attached to the product, while the smart card 108 is either attached to the product or simply packaged with the product. The legitimate manufacturer 101 make the public keys, 109 and 110, accessible to the customer or law enforcement agents 112, for instance through a link of the Internet World Wide Web (WWW) 111. The customer can verify authenticity in a first stage by examining the visible label using public key 109 or verification can be performed by the customer after the purchase by examining the hidden label using public key 110. The cashier may verify the authenticity of the product from the visible label in front of the customer with a point of sale (POS) machine 115 such as a cash register equipped with the appropriate public key and, if desired, a smart card reader.

The protection coming from the smart card containing the serial number and the private key/public key pair 104 and 110 can be omitted if the customer is satisfied with the level of authenticity verification provided by the visible label. Similarly, specific agents may only be interested verifying the smart card in which case the label can be omitted. Using the link to the WWW 111, or some other link to the legitimate originator, the customer may be able to

register the serial number of the product that has been purchased. After the customer initiates such initial contact, the manufacturer can contact the customer for example to relay product update information, recall information, etc.

The label and smart card composition and data can be further detailed as follows for a series of serial numbers with reference now to Figure 3. The product information 201, manufacturing information 202, routing information 203, and the previous serial number in the series (or some initialization number at first stage) 204 are sent to the serial number generator 205. The serial number is sent to private key number-2 at block 206. The encrypted versions of the serial number is sent to the smart card writer at block 209 which writes it on the smart card 211. The serial number is also sent by the serial number generator 205 to printer-1 at block 208, possibly in conjunction with an encrypted version of it, encrypted using private key number 1 at block 207. What is received at printer-1 208 is printed on the visible label 210. Controls are be made, using the public keys corresponding to private key-1, and if needed private key- 2, to verify that the label and the smart card 211 correspond to each other and, when private key-1 is used, that the readable and encoded versions of the serial number match on the visible label. Private key-1 (207) can be replaced by some apparatus generating a watermark or other alteration of the product which do not affect its quality in a human-perceptible way.

The visible label will be printed by a printer linked to a computer 213. A part of the serial numbers is composed in successive sequences incremented by one. A part of the serial number will preferably contain information such as

routing, product name, date, etc. Each serial number is processed by two private key encoders, yielding two numerical identifiers. One of the numerical identifiers is written to the smart card while the serial number and the second identifier are printed on the label, which will later be glued directly to the product or its packaging so as to be visible from the outside. The printing chain is also equipped with a verifier device (not shown) which checks that the various sets of numbers are printed in a synchronous way. The second numerical identifier allows a preliminary check of authenticity, which should enable easy identification of the more flagrant counterfeit product labeling.

Instead of a serial number, the numerical identifier could include a description of the physical appearance of the product, the color of the product, a chemical decomposition of the product and other descriptions of the product, including digital images of the product. This information will be contained in block 201 (Figure 3). Furthermore, the identifier could also be encoded in various forms of widely used barcodes.

A smart tag may be a smart card 211 or any other electronic device which contains memory and/or processing and computation circuitry and can operate autonomously and responds to queries from a verifying or authentication device. A more detailed discussion to smart card technology and applications can be found in "Smart Cards: a guide to building and managing smart card applications," by Henry Dreifus and J. Thomas Monk, John Wiley & Sons, 1998, herein incorporated by reference.

In case zero-knowledge protocols are used the smart card 211 is tamper resistant and/or duplication-resistant.

For certain applications, the smart card 211 may be programmed to self-destruct (i.e., erases its contents) after verification in which case the use of a visible label may be dispensed with. Alternatively, it could be kept and maintained as a title and record of the whole resale history of the product to which it is attached. Depending on applications, the smart card can contain only authentication information showing that the attached goods came from the purported manufacturer. For instance, the smart card can contain authentication information about the manufacturer, not the particular goods themselves, in which case the smart card is the same for all products by the manufacturer. In other applications, the smart card can further contain specific encrypted information about the attached goods, such as digital images of the goods, a physical or chemical description of the goods, unique serial numbers, etc. The verification procedure can be done using a card reader 215 equipped with the appropriate public key and zero-knowledge protocols to decrypt the identifying information. The card reader 215 may be required to make contact with the card 211 or, in certain applications where the card 211 is embedded in the goods, inductive, capacitive or some other type of contactless coupling may be employed by the reader to read the card 211.

Referring to Figure 4, this invention can be used to prevent parallel markets from occurring by encoding routing information into the serial number or in the coded version of it. At the point of sale, the customer can ask to authenticate the product, and this verification can only be done if the routing information is kept intact, and is compatible with the actual point of sale. The smart card reader which performs this authentication is designed to

only function in such circumstances. For example, the manufacturer give each merchant the routing information encrypted with a private key and the smart card reader can only authenticate the product if decrypting the encrypted routing information with a corresponding public key results in a match with the routing information on the product. In block 402, the smart card reader obtains the encrypted routing information from the merchant and decrypt it using a corresponding public key (403). In decision block 404 the decrypted routing information is compared with the routing information in the smart card. If they do not match, the product is not meant to be sold here and the authentication fails. If they do match, in decision block 405 the smart card is authenticated. If the smart card is not authenticated, the product fails to be authenticated. If the smart card is authenticated, in decision block 406, the product information in the smart card is compared with the serial number and/or other types of product information. If they do not match, the product is not authenticated. If they do match, the product is authenticated. As an additional incentive for the customer to perform such verification, one can decide that the warranty on a product can only be activated if the product can be authenticated in this way at the point of sale. Upon activation, the customer can choose to obtain a printed version of the warranty. If desired, the merchant can write onto a special memory section of the smart card the date and other information of the purchase.

While the invention has been described in terms of a preferred embodiment, those skilled in the art will recognize that the invention can be practiced with modification within the spirit and scope of the appended